FortiClient iOS - User Guide

Version 6.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

November 28, 2018
FortiClient iOS 6.0 User Guide
04-601-481912-20181128

TABLE OF CONTENTS

Introduction **4**
FortiClient iOS features 4
SSL DNS server for split tunnel 4
Supported platforms 5
Initial Configuration **6**
Running FortiClient iOS 6
Mobileconfig profile 9
Web Filtering 11
FortiTelemetry 14
User Profile 15
Enterprise Mobility Management **18**
AirWatch Integration 18
Jamf integration 23
Logs **29**
Change Log **31**

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This guide describes how to install and set up FortiClient iOS for the first time.

FortiClient iOS features

Feature	Description
SSL VPN (Tunnel Mode)	SSL VPN in Tunnel Mode supports the following: • IPv4 Example: `https://24.1.20.17` • IPv6 Example: `https://[1002:470:71f1:63::2]` • Full tunnel & split tunnel (IP and subnet based) • SSL realm, custom DNS server, DNS suffix • Username & password authentication • PKI user with a personal certificate, FortiToken & Client Certificate
Web Filter	All browser traffic is supported.
FortiTelemetry	Connect to FortiGate and FortiClient EMS for central management.
mobileconfig	Use the mobileconfig file to pre-configure a FortiClient Telemetry preferred host. Once FortiClient starts, it uses this preferred host to connect.
FortiAnalyzer support	Send logs to FortiAnalyzer when configured from FortiClient EMS. See the *FortiClient EMS Administration Guide*.

SSL DNS server for split tunnel

To use the SSL DNS server for split tunnel, the DNS suffix must be configured on the FortiGate side. Following is an example of configuring SSL DNS server for split tunnel using FortiOS:

```
config vpn ssl settings
   set dns-suffix
"domain1.com;domain2.com;domain3.com;domain4.com;domain5.com;domain6.com;domain7.com;domain8.c
      om"
   set dns-server1 10.10.10.10
   set dns-server2 10.10.10.11
```

```
config vpn ssl web portal
   edit "full-access"
      set dns-server1 10.10.10.10
      set dns-server2 10.10.10.11
      set split-tunneling enable
```

If the split tunnel is configured, only DNS requests that match DNS suffixes use the DNS servers configured in the VPN. Due to iOS limitations, the DNS suffixes are not used for search as in Windows. Using short (not FQDN) names may not be possible.

Supported platforms

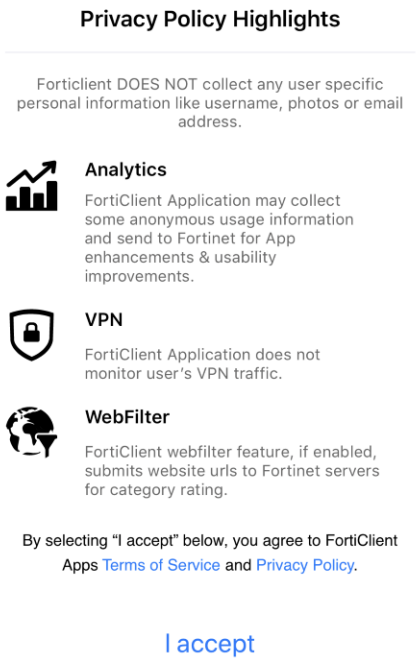
FortiClient iOS is supported by iOS versions 9, 10, 11, and 12.

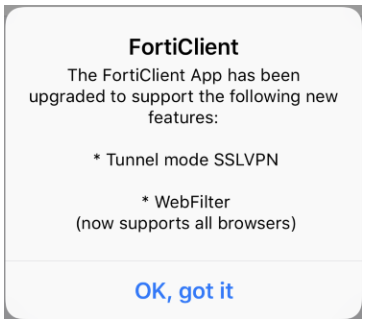
Initial Configuration

The following sections provide instructions on initial configuration of FortiClient iOS:

Running FortiClient iOS

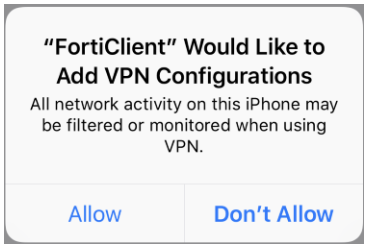
After downloading the FortiClient installer and running the application for the first time, you must acknowledge some popups before continuing to add a VPN configuration. Acknowledge the notifications shown below.





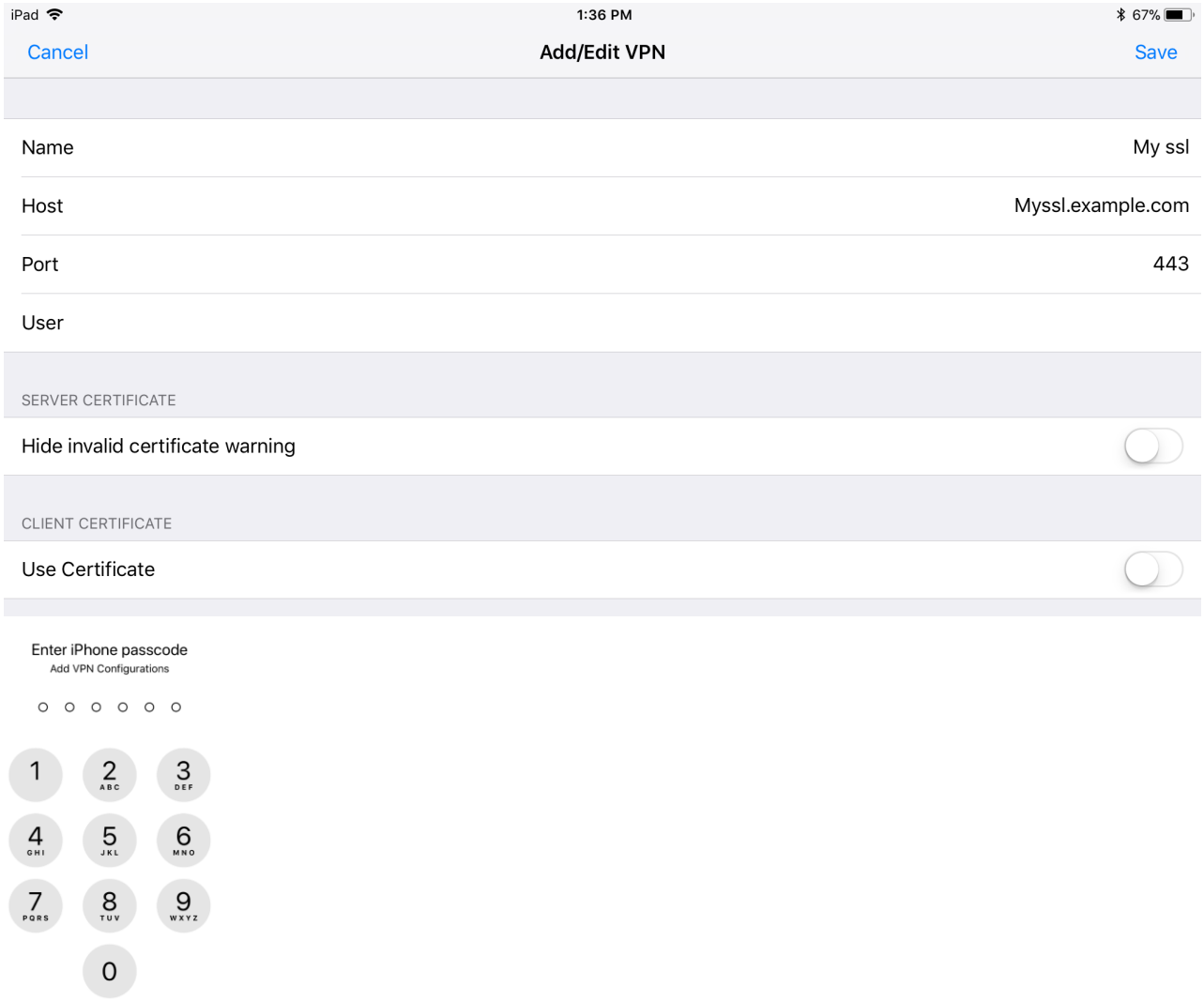
To add a VPN connection:

1. In the *Add VPN Configurations* popup, tap *Allow*.



2. Tap the *VPN* icon at the bottom of the screen to switch to the VPN page.

3. Tap *Connections* > *Edit* > *Add Configuration*, then configure the following. Enter your passcode to confirm adding the VPN.

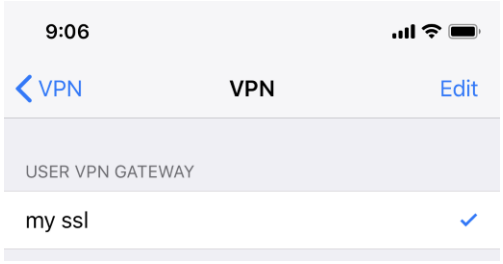


4. Tap *Done* twice.

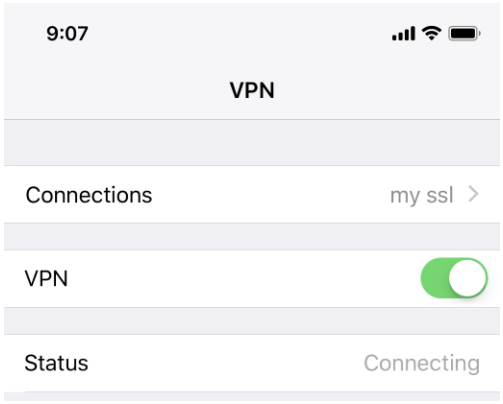
The *Name*, *Host* and *Port* fields are required. The *User*, *Hide invalid certificate warning*, and *User Certificate* fields are optional.

To enable a VPN connection:

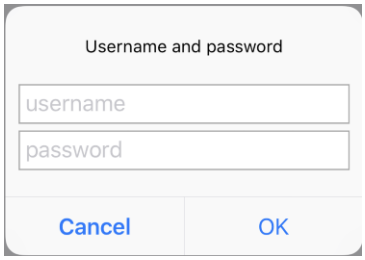
1. Tap a *VPN connection*. A checkmark appears beside the VPN connection to indicate it is selected.



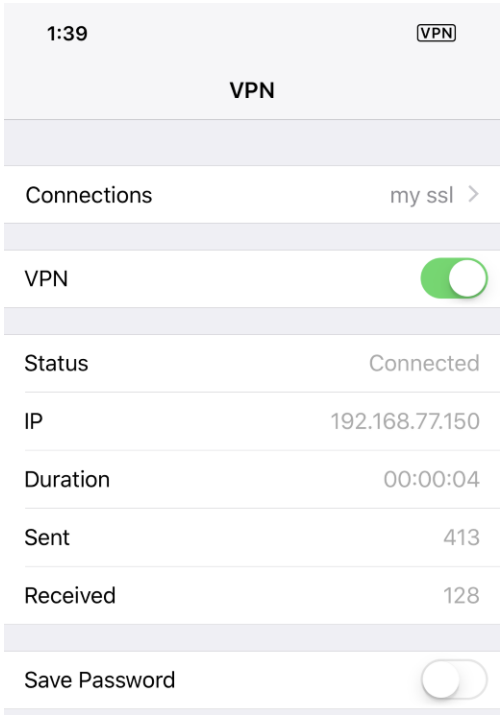
2. Tap the < button.
3. Swipe right to enable the VPN connection.



4. If the username and password are not configured, enter the *username and passcode* in the popup.



5. Tap *OK*. When connected, the tunnel interface IP, duration, and the bytes sent and received information display.



To disable a VPN connection:

1. Select the VPN connection.
2. Swipe left to disable the VPN connection.

To edit or delete a VPN connection:

1. Select a VPN connection.
2. Tap *Edit* or *Delete*.
3. Tap *Done* twice.

Mobileconfig profile

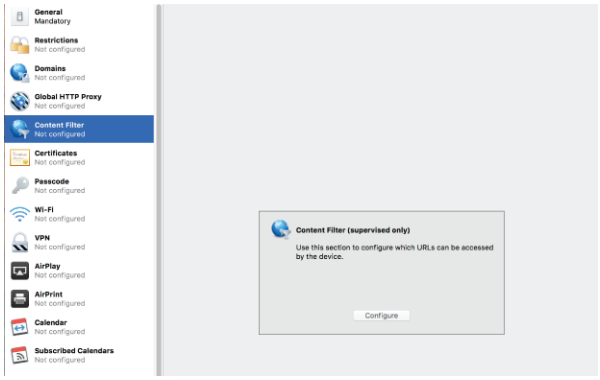
To enable web filtering, the iOS device must be supervised and a Mobileconfig profile with a content filter must be installed on the device. The following is required to install a mobileconfig profile:

1. Apple Configurator 2 (or equivalent Mobile Device Management application) installed
2. iOS devices are supervised

Instructions on how to supervise your iOS devices can be found on the Apple Configurator 2 Help (or your MDM application) website.

To create a mobileconfig profile for FortiClient web filtering:

1. Launch *Apple Configurator 2*.
2. Go to *File* > *New Profile*.
3. Enter a *Name* for the profile.
4. Select *Content Filter* from the left panel.



5. Click *Configure*.
6. Select *Plugin (Third Party App)* from the *Filter Type* dropdown list.
7. Configure the following:

Filter Name	FortiClient
Identifier	com.fortinet.forticlient
Service Address	fgd1.fortigate.com
Organization	Fortinet, Inc.
User Name	You can use this field to specify EMS server (IP or FQDN), port, and connection key (optional). For example, for following string will allow FortiClient iOS to connect to EMS server at ems.example.com at port 8013, with key “ConnectionKey”: ems.example.com:8013 ConnectionKey
Filter WebKit Traffic	Select the *Filter WebKit Traffic* checkbox.
Filter Socket Traffic	Select the *Filter Socket Traffic* checkbox.

8. Click *Save*.

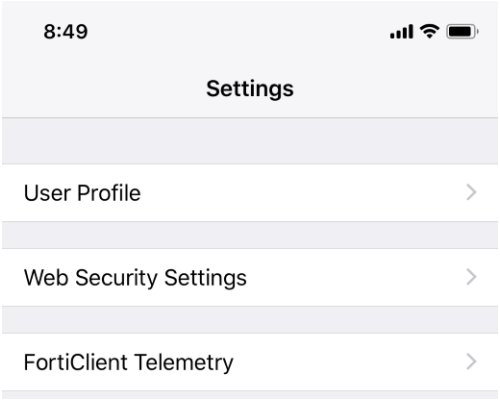
Due to restrictions set by Apple, FortiClient iOS must be launched once before the configuration can take effect. You can use FortiGate compliance enforcement to ensure users launch FortiClient iOS before browsing the Internet. For details, see *FortiClient Compliance Profiles* in the *FortiOS Handbook*.

Web Filtering

Web Filtering is disabled by default. To enable Web Filtering, the iOS device must be supervised and a Mobileconfig profile with a content filter must be installed on the device. See Mobileconfig profile.

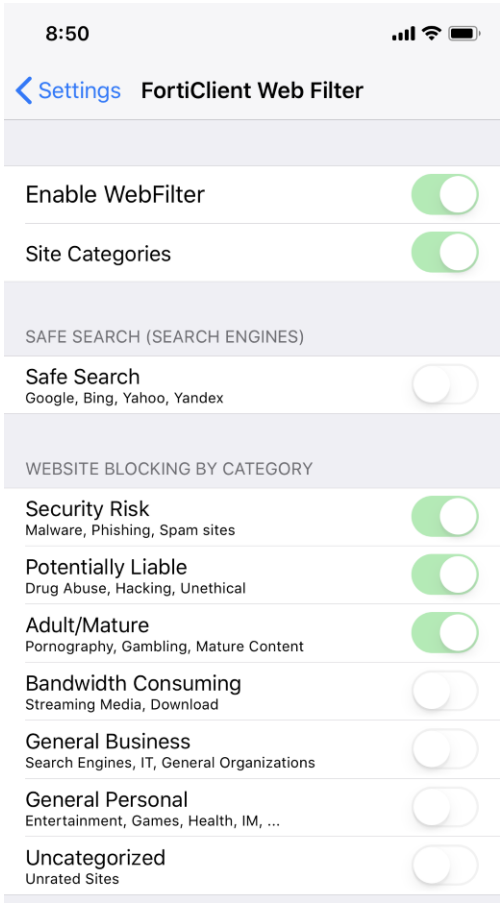
To configure the Web Filtering settings:

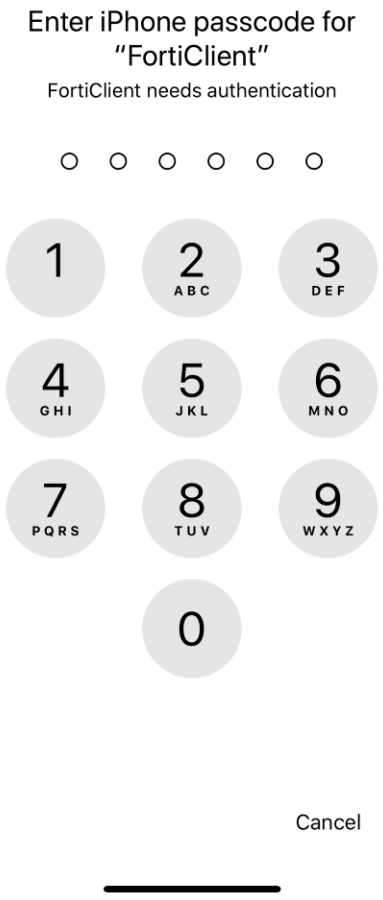
1. Tap *Settings*.
2. Tap *Web Security Settings*.



3. Enter the passcode in the *FortiClient Authentication* popup.
4. Enable the *Web Filter* by swiping right.

5. Configure the *Website Blocking by Categories* to suit requirements.



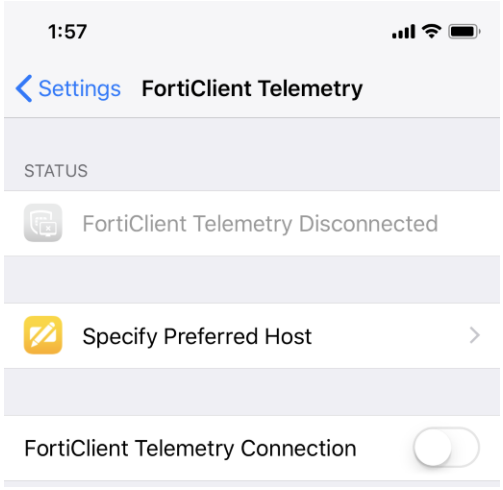


When a website is blocked, a restricted website error page appears.

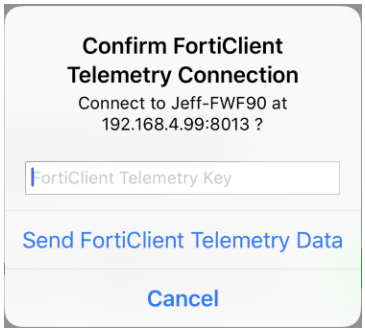
FortiTelemetry

To configure the FortiClient Telemetry settings:

1. Tap *Settings* at the bottom of the screen.
2. Tap *FortiClient Telemetry*.



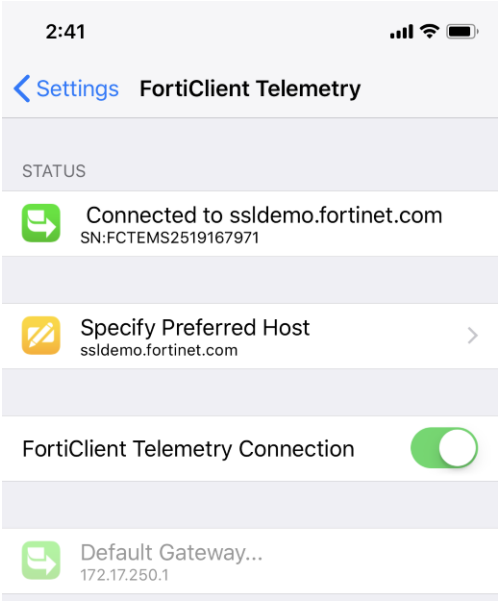
3. Enable *FortiClient Telemetry* by swiping right. When FortiClient detects a FortiTelemetry server, a confirmation pop up window will appear.



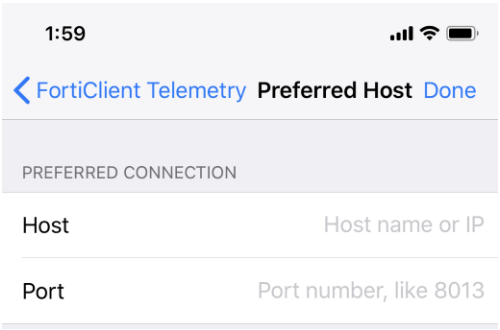
4. Tap *Send FortiClient Telemetry Data* to connect to the FortiTelemetry server.

To specify a FortiTelemetry server:

1. Tap *Specify Preferred Host*.



2. Enter *Host* and *Port*.



3. Tap *Done*.

You can use the mobileconfig file to preconfigure a FortiClient Telemetry preferred host. Once FortiClient starts, it uses this preferred host to register. See Mobileconfig profile on page 9.

User Profile

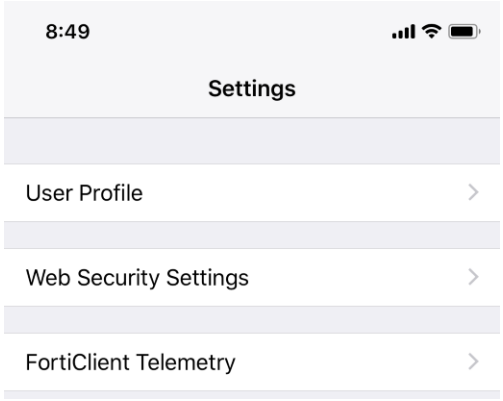
You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- LinkedIn
- Google
- Facebook

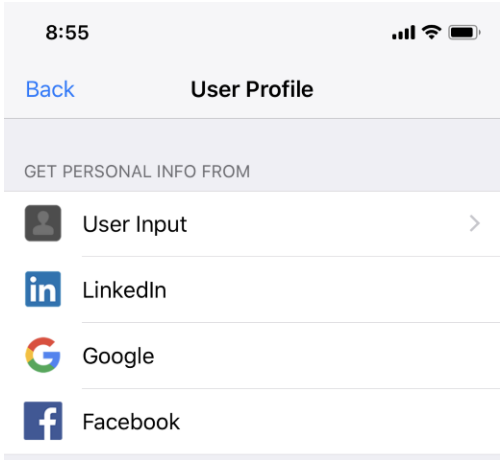
You can also manually add or edit a name, phone number, and email address in FortiClient. This user data is sent to FortiClient EMS, where it is displayed on the *Endpoints* content pane.

To retrieve user details from a cloud application:

1. Tap *Settings* at the bottom of the screen.
2. Tap *User Profile*.



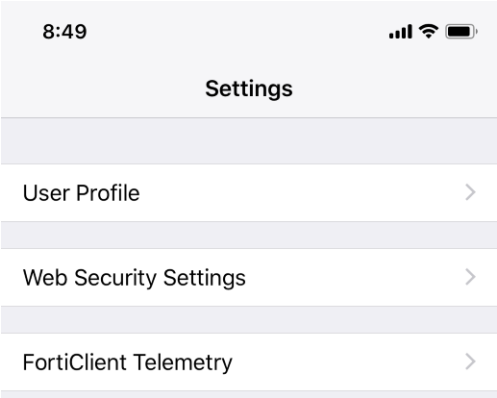
3. Tap the desired cloud application.



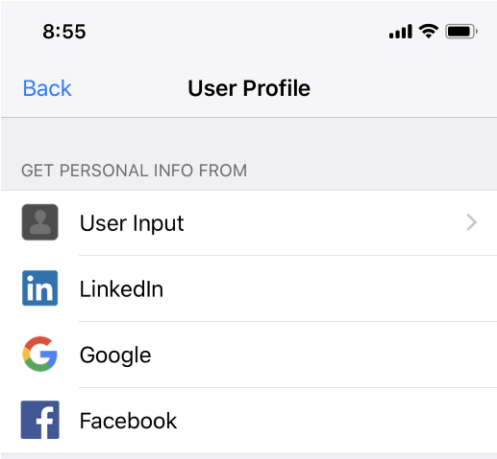
4. If you are not logged into the cloud application already on this device, you must log in. Grant FortiClient iOS permission to use your information.

To add user details manually:

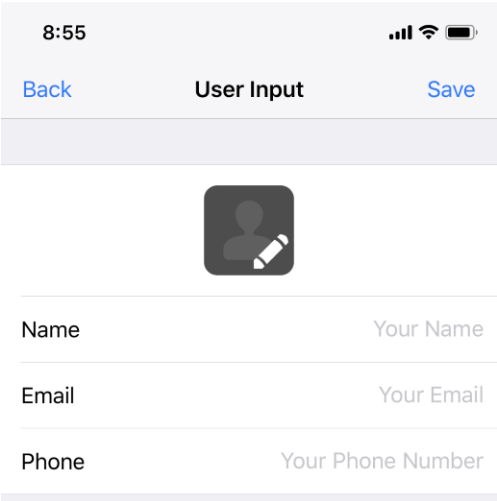
1. Tap *Settings* at the bottom of the screen.
2. Tap *User Profile*.



3. Tap *User Input*.



4. Tap to edit the photo, name, email, and phone number as desired.



5. Tap *Save*.

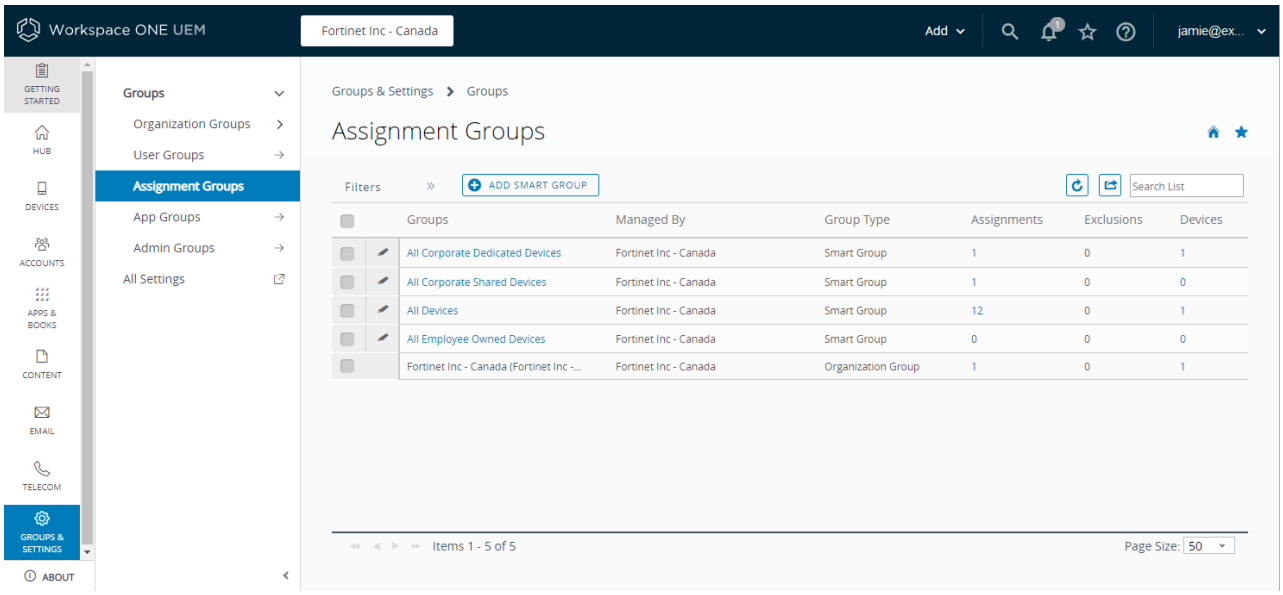
Enterprise Mobility Management

FortiClient iOS supports integration with enterprise mobility management software including AirWatch and Jamf. Integration with AirWatch or Jamf allows FortiClient iOS endpoints to connect to EMS. Mobile device management through Jamf and AirWatch is only supported for FortiClient iOS 6.0.1 and later versions.

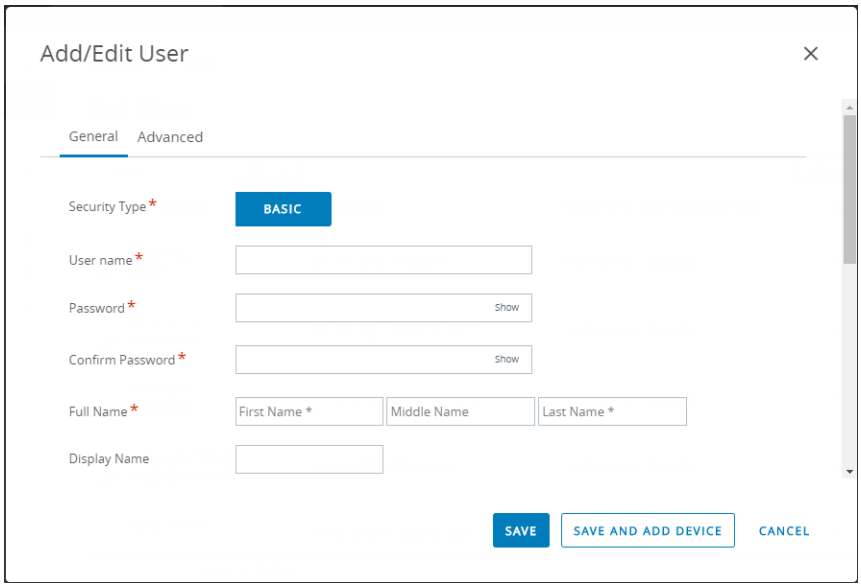
AirWatch Integration

The following describes how to configure integration between AirWatch and FortiClient iOS. Integration with AirWatch allows FortiClient iOS endpoints to connect to EMS.

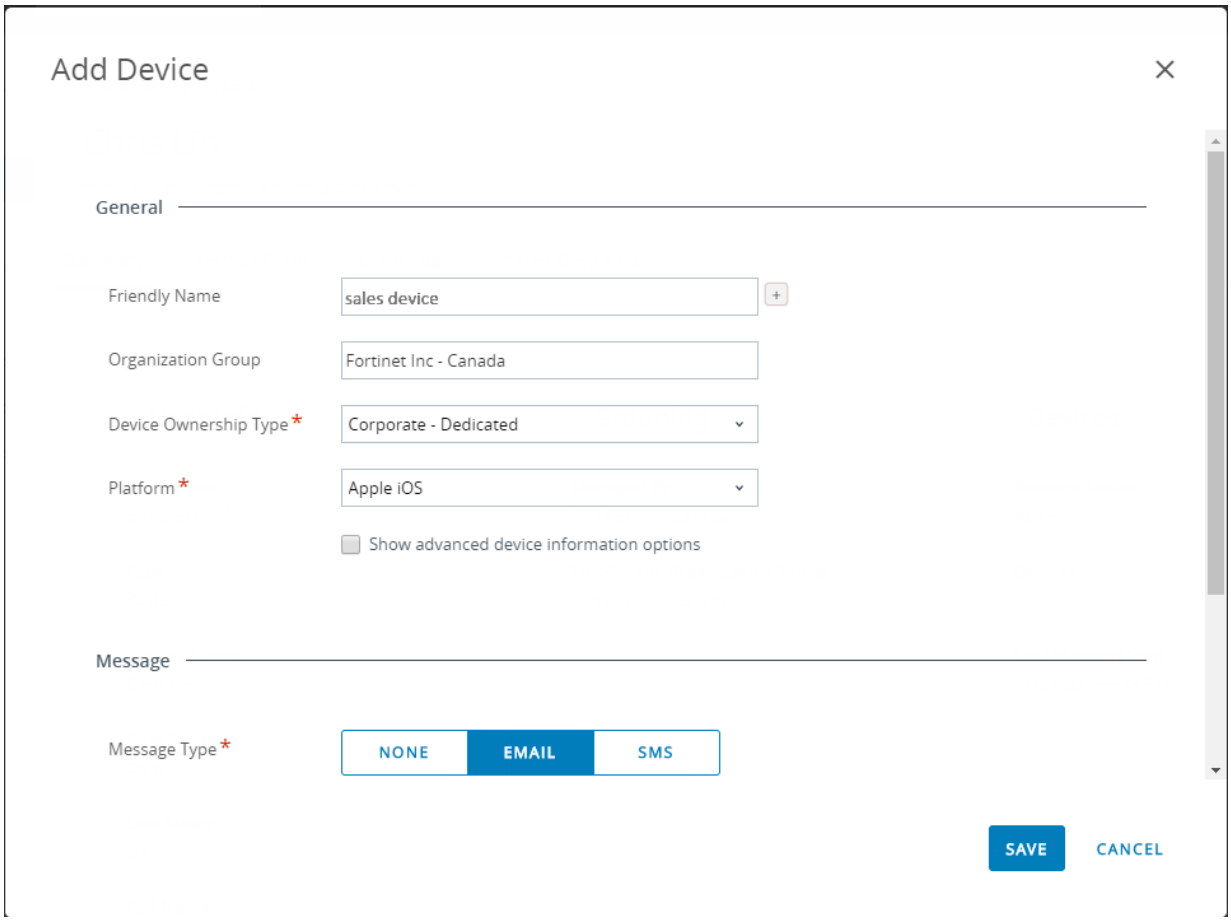
1. In AirWatch, navigate to *Groups & Settings* > *Assignment Groups*. Create a new assignment group.



2. Navigate to *Accounts*, and add a new user.

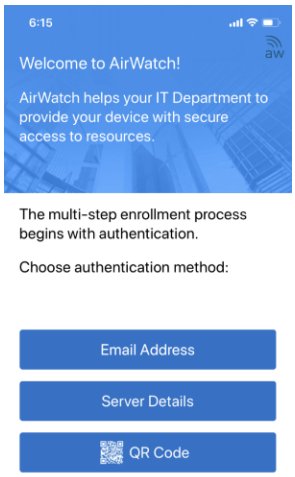


3. Add a new device for the user:
   a. From the *Device Ownership Type* dropdown list, select *Corporate - Dedicated*.
   b. From the *Platform* dropdown list, select *Apple iOS*.
   c. For *Message Type*, select *EMAIL*.

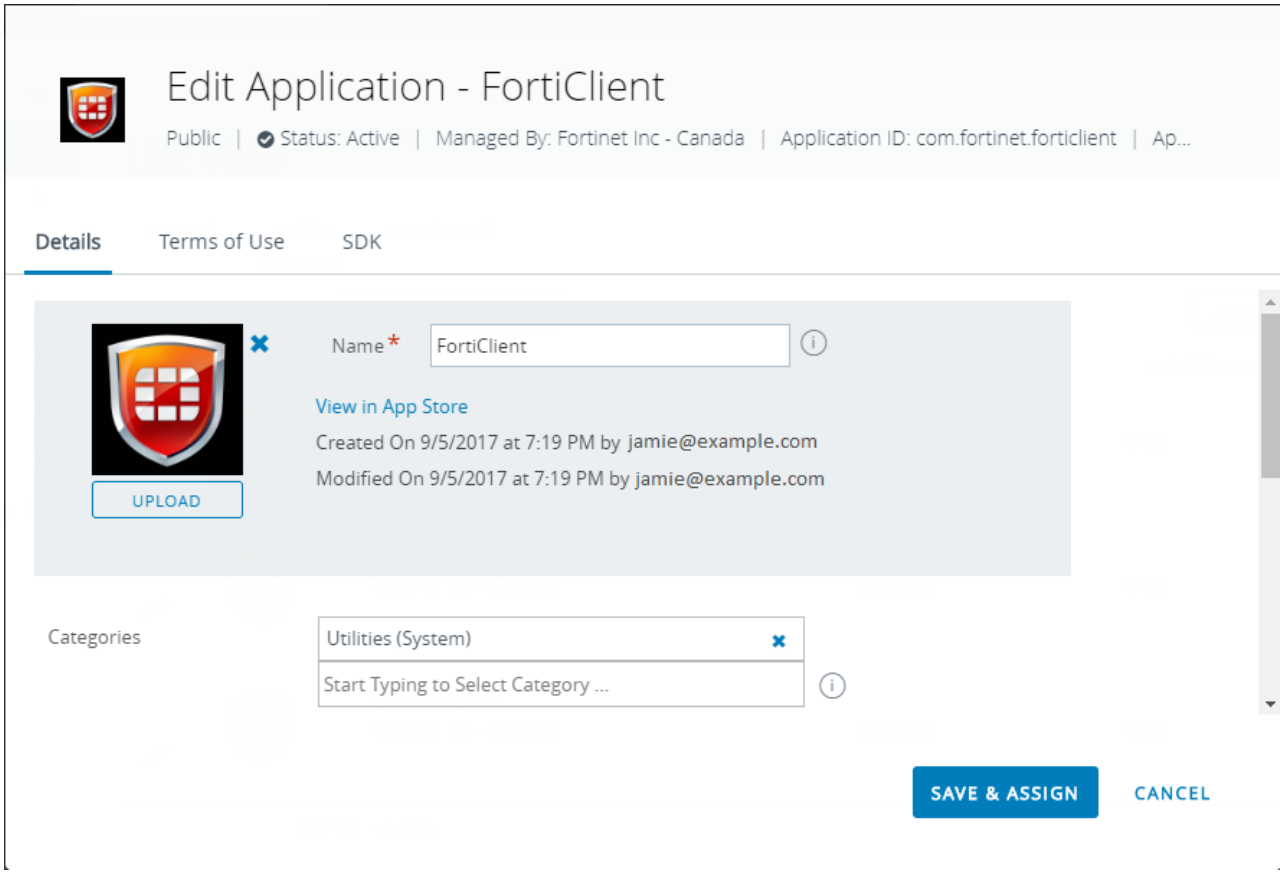


d. Save. This sends an AirWatch device activation email to the user.

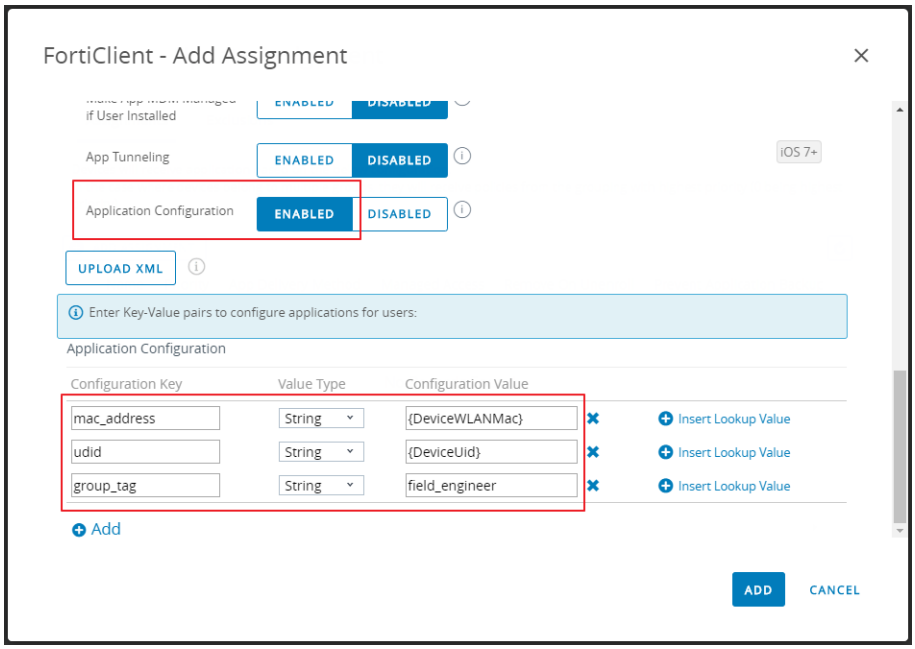
4. The user installs AirWatch agent on the device and scans the QR code in the activation email to enroll the device.



5. In AirWatch, go to *Apps & Books*, and add FortiClient iOS from the public App Store.

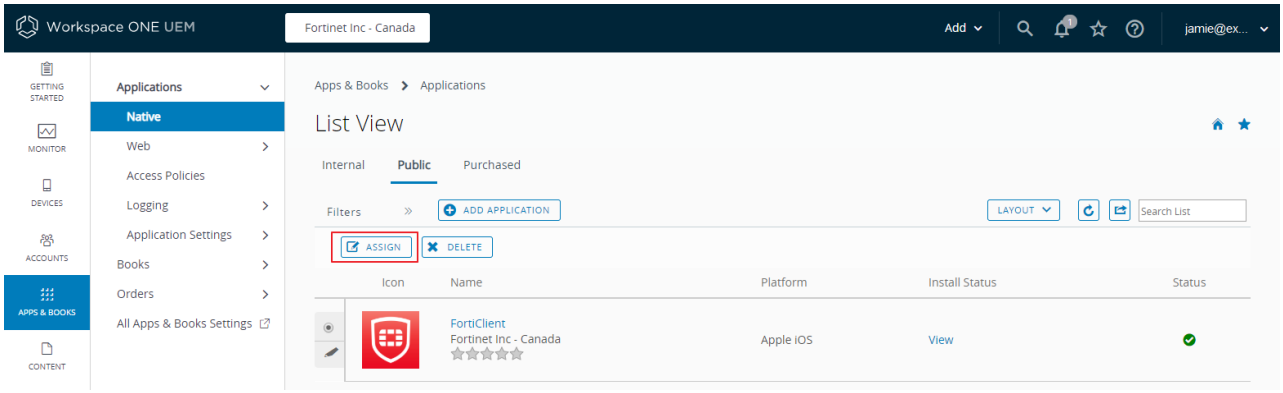


6. When adding an assignment, scroll to the bottom and enable *Application Configuration*. Optionally, you can add key-value pairs as shown.

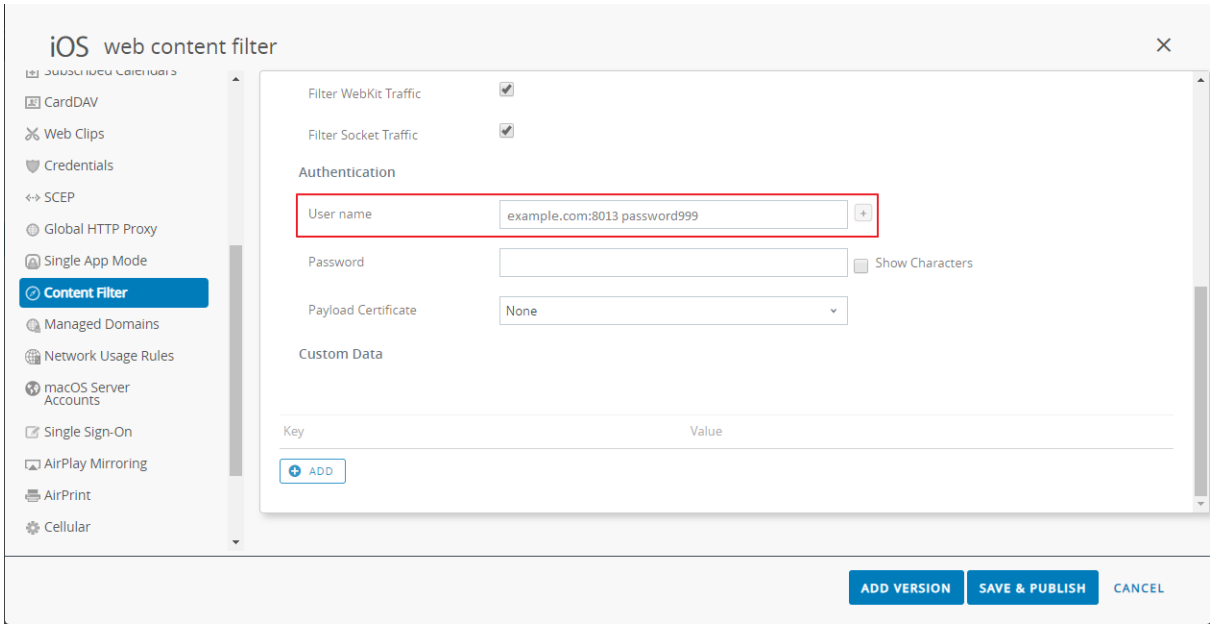


Supported keys include mac_address, udid, and group_tag. Using the key-value pairs shown above enables FortiClient iOS to read the MAC address and UDID from the iOS device. In this example, the string "field_engineer" is used as a group tag, which will be used when FortiClient iOS initially connects to EMS. See *Group assignment rules* in the *FortiClient EMS Administration Guide*.

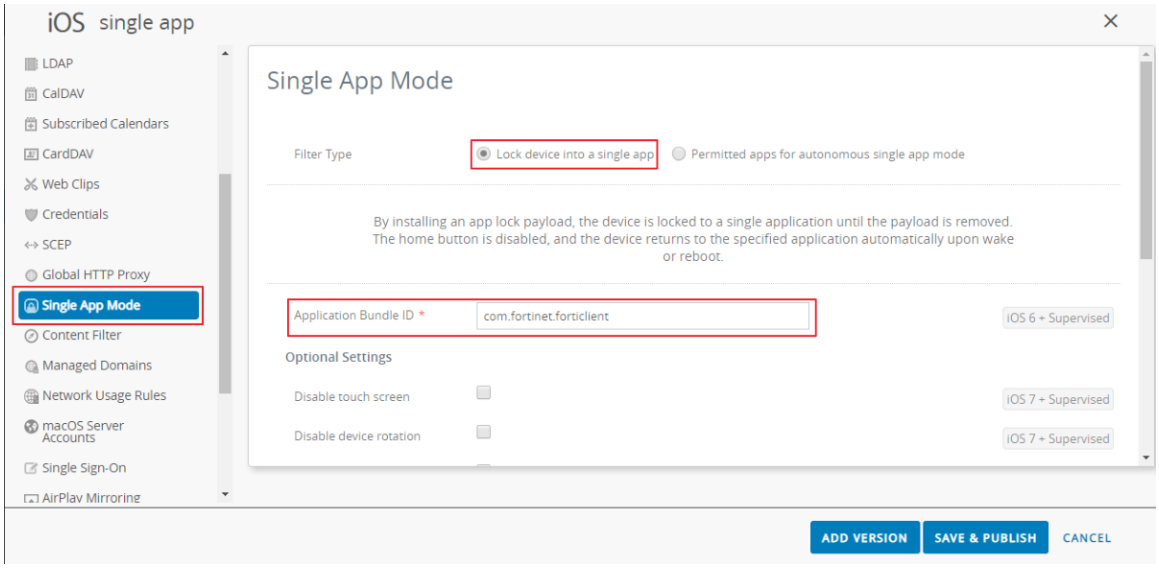
7. You can add more assignments and use different group_tag values.



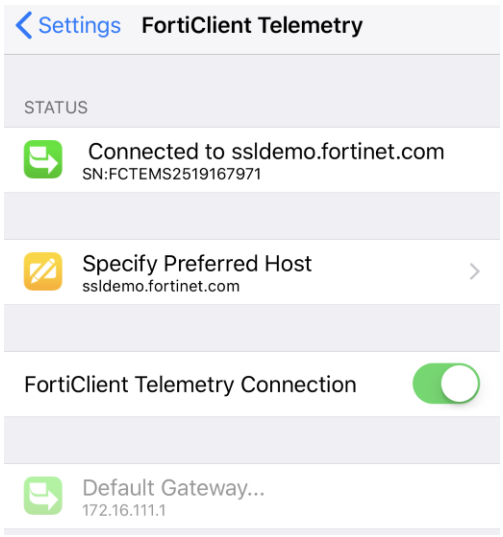
8. Go to *Devices*, and add a profile.
   a. Go to the *Content Filter* section. In the *User name* field, enter the EMS URL.



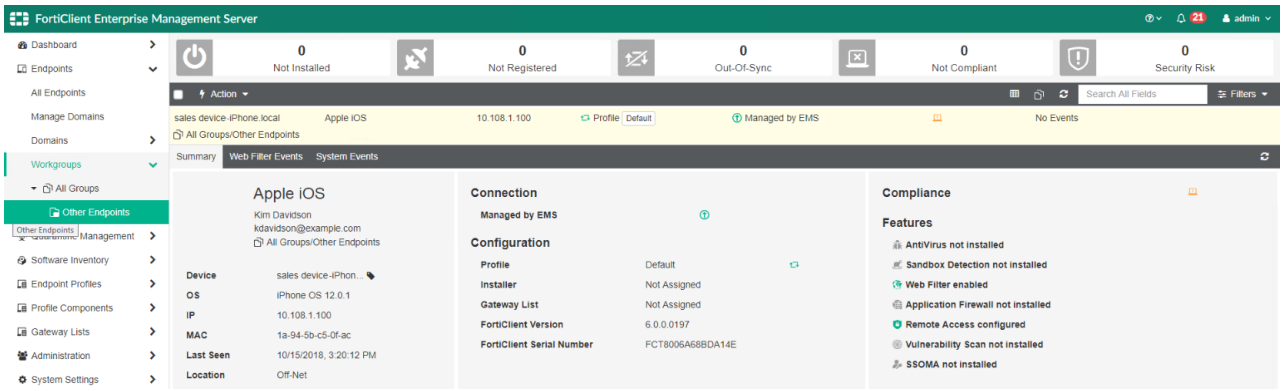
   b. Go to *Single App Mode*, and configure as shown below to enable single app mode. This makes FortiClient iOS run.



   c. Assign the profile to the device.
9. When FortiClient is started on the device, it automatically connects to EMS. Once FortiClient is connected to EMS, disable single app mode for the device. Keep the EMS URL in the *Content Filter* section.



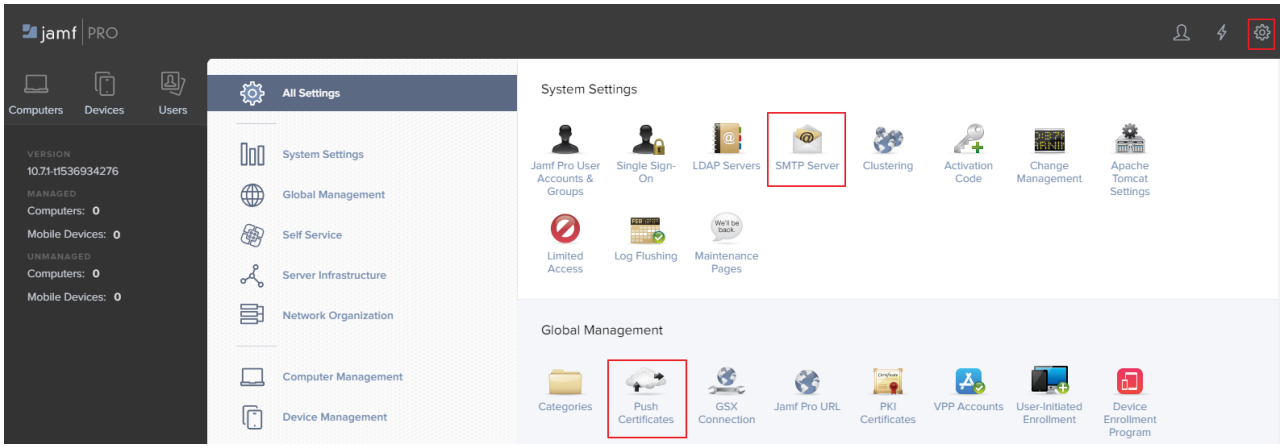
The below shows the EMS GUI after FortiClient iOS connects Telemetry.



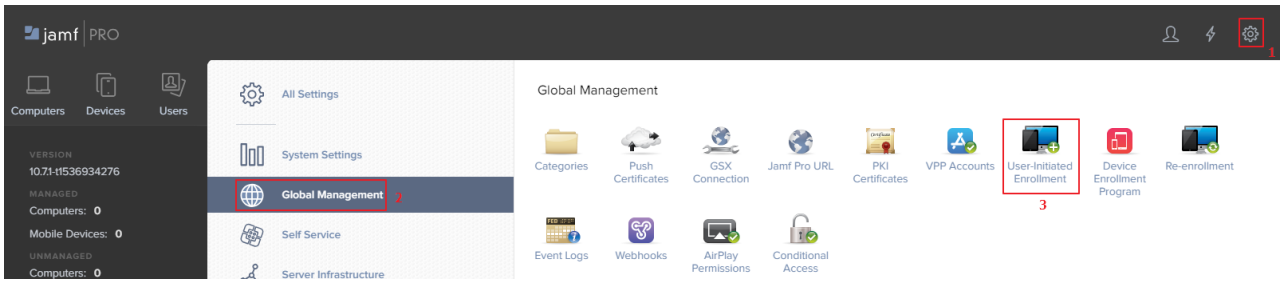
Jamf integration

The following describes how to configure integration between Jamf and FortiClient iOS.

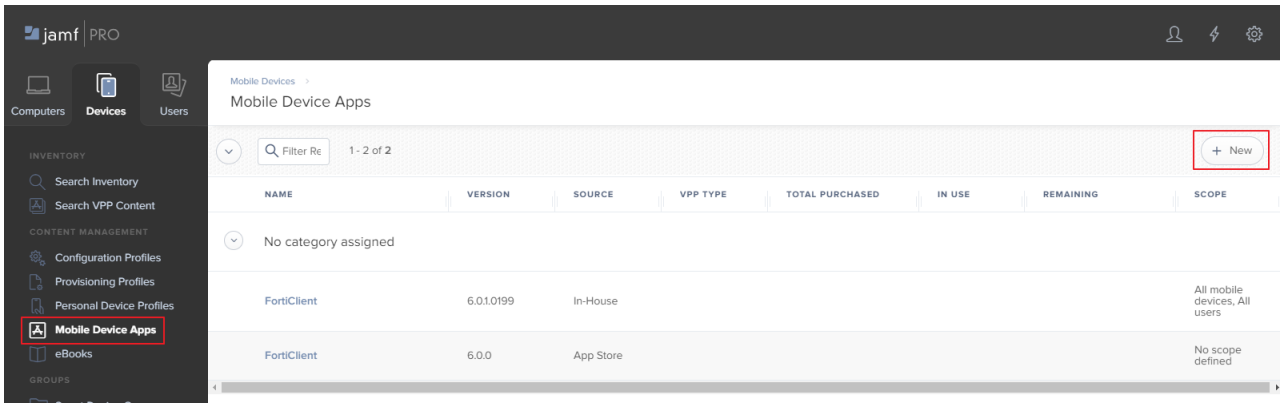
1. In Jamf, navigate to *All Settings*. Configure the settings in *SMTP Server* and *Push Certificates*.



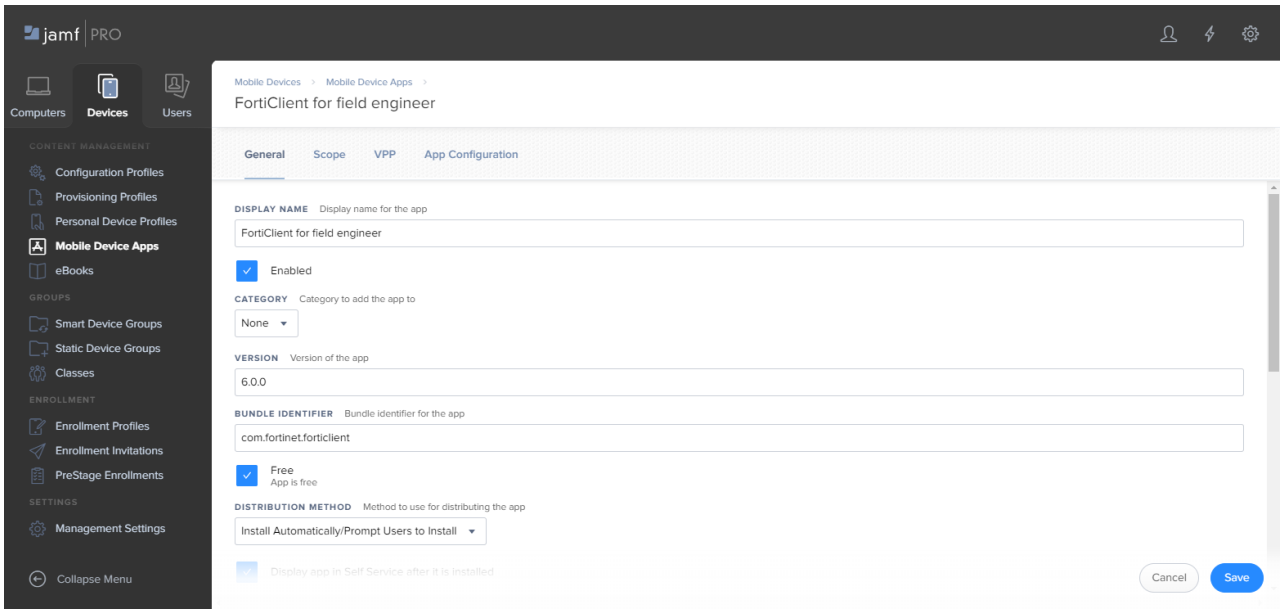
2. Navigate to *Global Management*, and enable *User-Initiated Enrollment*.



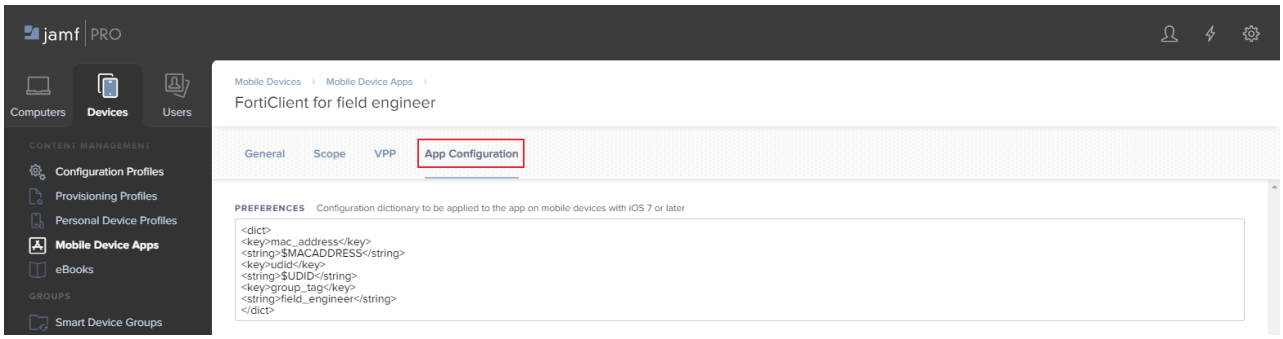
3. Go to *Mobile Device Apps* and add FortiClient from the App Store or by uploading it.



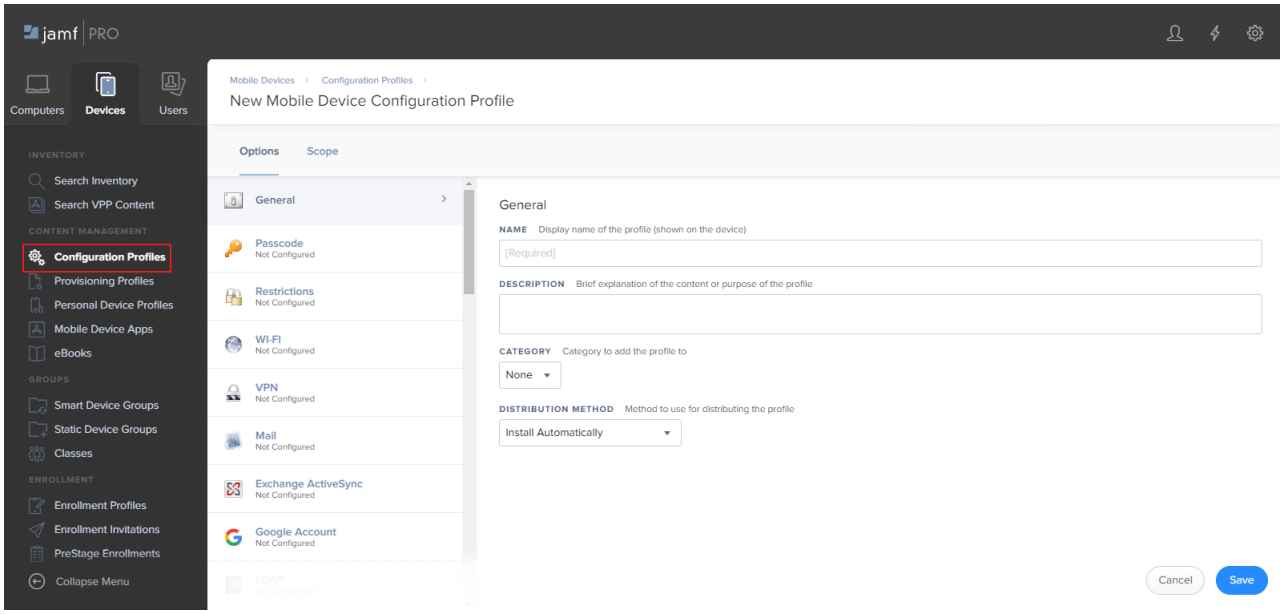
4. Configure how the app is installed.



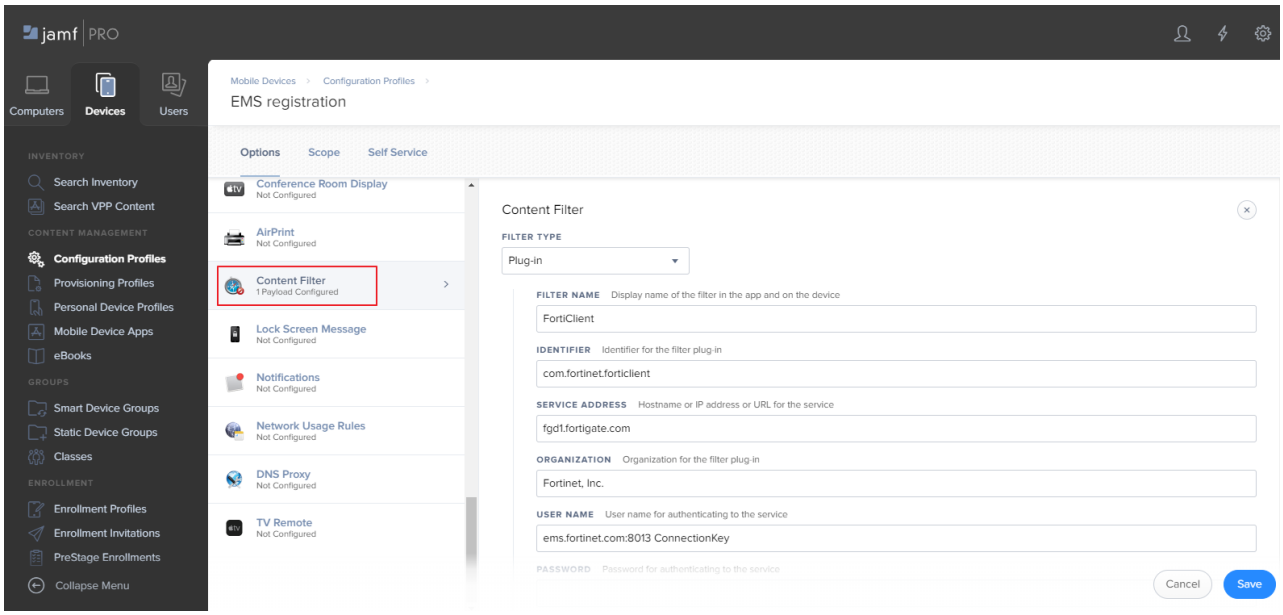
5. Add *App Configuration* for FortiClient iOS. This enables FortiClient iOS to read the MAC address and UDID from the iOS device. In this example, the string "field_engineer" is used as a group tag, which will be used when FortiClient iOS initially connects to EMS. See *Group assignment rules* in the *FortiClient EMS Administration Guide*.



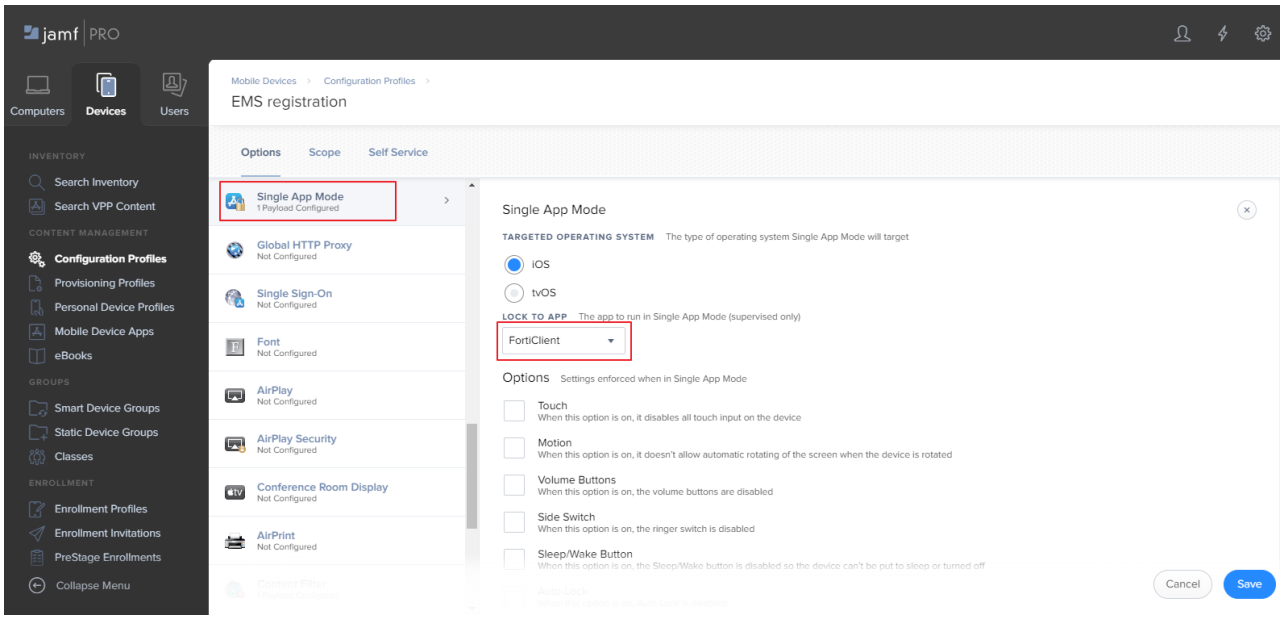
6. Go to *Configuration Profiles* and add a configuration profile.



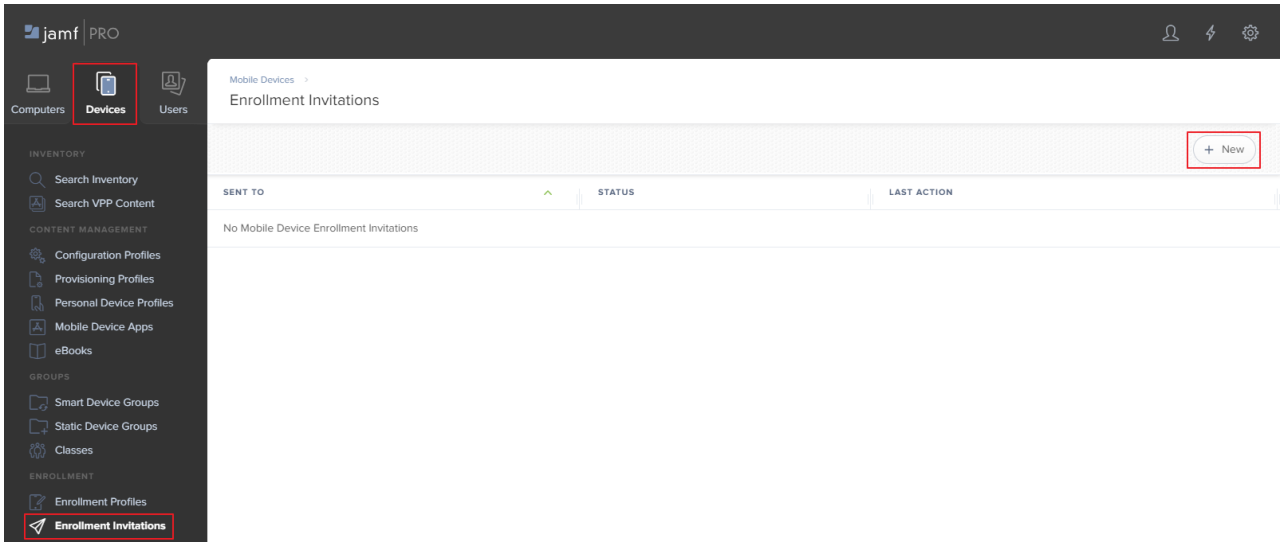
7. Under *Options*, select *Content Filter*. Add a content filter to point to the desired EMS.



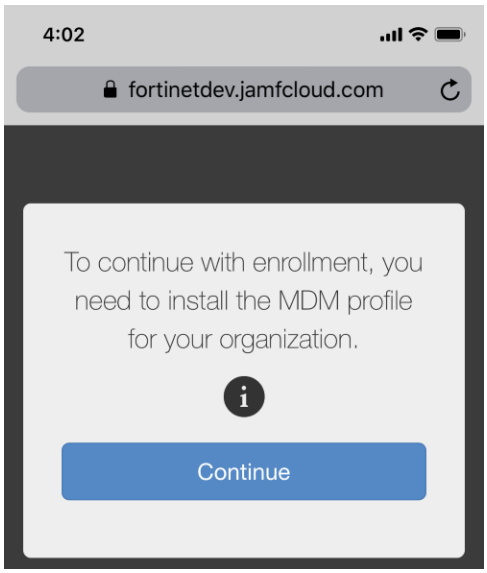
8. Enable *Single App Mode* for FortiClient. Single app mode launches the FortiClient app and connects it to EMS. If FortiClient is not launched in single app mode, it does not connect to EMS.

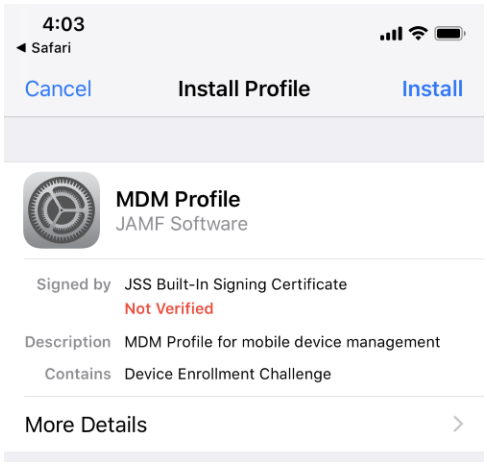


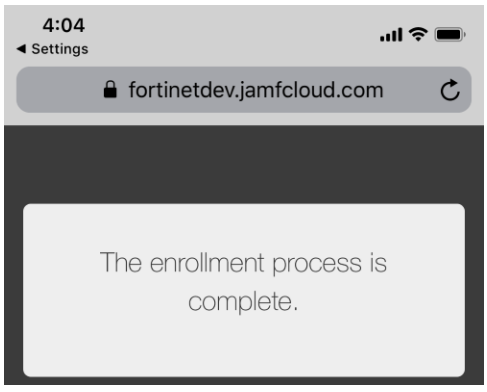
9. Go to *Devices* > *Enrollment Invitations*, then send an enrollment invitation to the device.



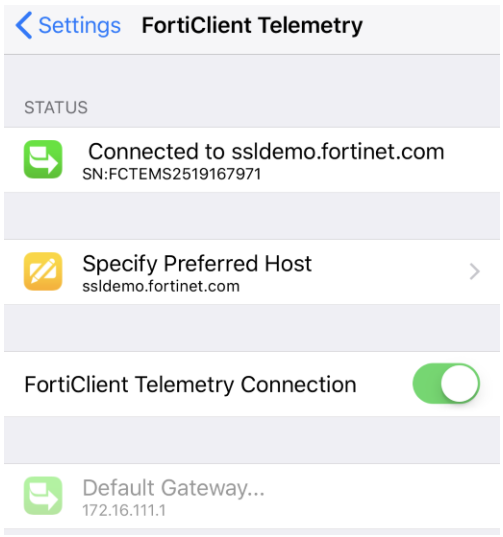
10. Enroll the device.



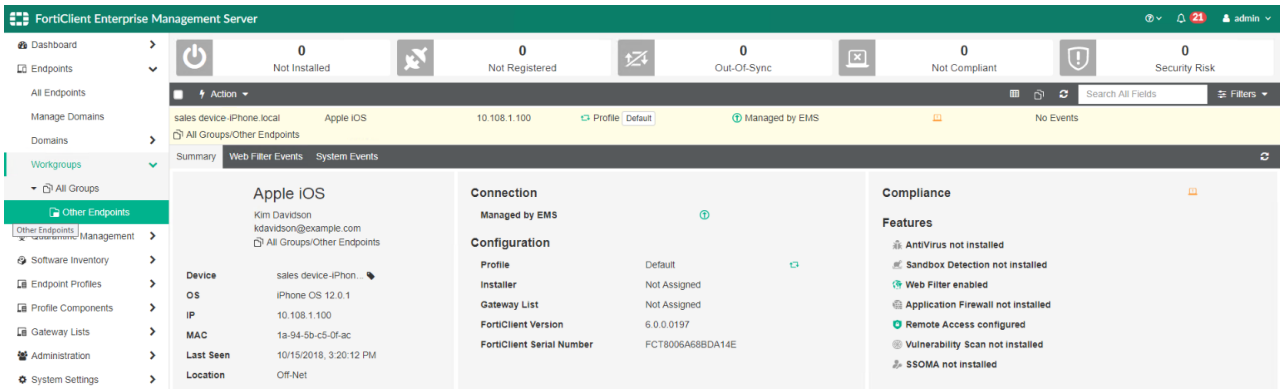




11. When the device is enrolled, Forticlient automatically connects to EMS. Once FortiClient is connected to EMS, disable single app mode for the device. Keep the EMS URL in the *Content Filter* section.



The below shows the EMS GUI after FortiClient iOS connects Telemetry.

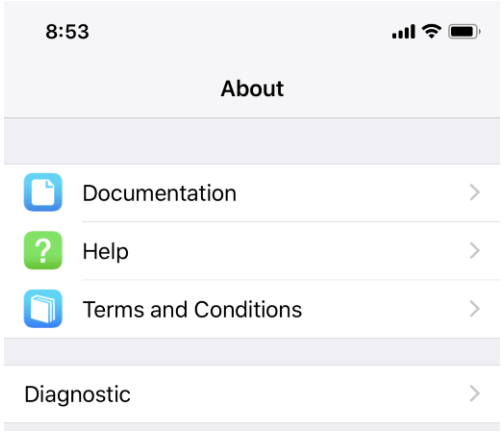


Logs

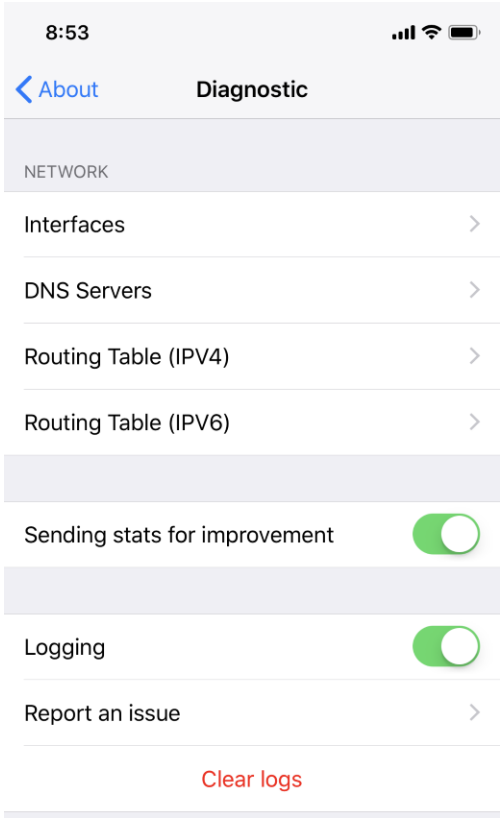
You can email FortiClient iOS logs to Fortinet.

To email logs to Fortinet:

1. Tap *About*.
2. Tap *Diagnostic*.



3. Swipe right to enable *Logging*.



4. Tap *Email Logs*.

Change Log

Date	Change Description
2018-09-25	Initial release.
2018-10-16	Added AirWatch Integration on page 18.
2018-11-28	Release of FortiClient iOS 6.0.1. Added Jamf integration on page 23 and added MAC address and UDID detail for AirWatch Integration on page 18.